08-08-05

$ AF
JFW

PATENT

I HEREBY CERTIFY THAT ON THE DATE SHOWN BELOW, THIS CORRESPONDENCE IS BEING DEPOSITED WITH THE U.S. POSTAL SERVICE IN AN ENVELOPE ADDRESSED TO: COMMISSIONER FOR PATENTS, P.O. BOX 1450, ALEXANDRIA, VA 22313-1450, AS "EXPRESS MAIL POST OFFICE TO ADDRESSEE" MAILING LABEL NO. ET694209026US

ON AUGUST 5, 2005

Lisa L. Pringle

SIGNATURE LISA L. PRINGLE

THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	:	Kenneth Aull
Serial No.	:	09/823,701
Filing Date	:	March 30, 2001
For	:	PREVENTING ID SPOOFING WITH UBIQUITOUS SIGNATURE CERTIFICATES
Group Art Unit	:	2137
Examiner	:	Kevin R. Schubert
Attorney Docket No.	:	NG(MS)7185

Mail Stop Appeal Briefs - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

08/08/2005 SDENBOB1 00000074 09823701

01 FC:1402 500.00 OP

APPEAL BRIEF

Sir:

Pursuant to the Notice of Appeal filed in this case on May 4, 2005, Appellant's present herewith their Brief on appeal.

I. REAL PARTY IN INTEREST

The real party in interest is Northrop Grumman Corporation, as indicated by the Assignment recorded August 11, 2004, Reel/Frame: 013751/0849.

II. RELATED APPEAL AND INTERFERENCES

There are no related appeals or interferences.

III. STATUS OF CLAIMS

Claims 1-16 are rejected.

Claims 1, 5, 9 and 13 are appealed.

IV. STATUS OF AMENDMENTS

No amendments of the claims were filed after the Final Rejection, dated March 7, 2005.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

A. Summary of Independent Claims 1 and 9

Claims 1 and 9 are directed to a method and apparatus (Para. [0013]) of preventing ID spoofing of a public key infrastructure system in an enterprise (100 of FIG. 1) comprising: allowing a user to access a registration server (Para. [0031]) (124 of FIG. 3); upon the registration server receiving identification information from the user and also receiving a request by the user for a new signature certificate, the registration server querying a directory (108 of FIG. 3) containing reference information of users of the enterprise to obtain information regarding the identified user (Para. [0031]); and upon the registration server receiving information from the directory indicating that the identified user already possesses a signature certificate, the registration server informing the user that a new signature certificate will not be issued until the old signature certificate has been revoked (Para. [0031]), thereby preventing an unauthorized user (236 of FIG. 3) from ID spoofing to obtain a valid signature certificate and maintaining a one-to-one correspondence between users of the enterprise and signature certificates (Para. [0028]).

B. Summary of Independent Claims 5 and 13

Claims 5 and 13 are directed to a method and apparatus (Para. [0014]) of preventing ID spoofing of a public key infrastructure system in an enterprise (100

of FIG. 1) comprising allowing a user to access a registration server (Para. [0034]) (124 of FIG. 3); upon the registration server receiving identification information from the user and also receiving a request by the user for a new signature certificate, the registration server querying a directory (Para. [0034]) (108 of FIG. 3) containing reference information of users of the enterprise to obtain information regarding the identified user; and upon the registration server receiving information from the directory indicating that the identified user is not in the directory, the registration server informing the user that a signature certificate will not be issued (Para. [0034]), thereby preventing an unauthorized user (236 of FIG. 3) from ID spoofing to obtain a valid signature certificate and maintaining a one-to-one correspondence between users of the enterprise and signature certificates (Para. [0028]).

VI. GROUNDS OF REJECTION TO BE REVIEW ON APPEAL

1. Whether claims 1 and 9 are anticipated by U.S. Patent No. 5,878,138 (hereinafter, "Yacobi")?

2. Whether claim 5 and 13 are anticipated by U.S. Patent No. 5,878,138 (hereinafter, "Yacobi")?

VII. ARGUMENTS FOR CLAIMS 1, 5, 9 AND 13

The United States Court of Appeals for the Federal Circuit ("Federal Circuit") has held that, "anticipation requires the disclosure in a single prior art reference of each element of the claim under consideration." *W.L. Gore & Assocs. v. Garlock*, 721 F.2d 1540, 220 U.S.P.Q. 303 (Fed. Cir. 1983).

1. 35 U.S.C. §102(b) rejection of claims 1 and 9 as being anticipate by Yacobi

Yacobi does not explicitly or inherently disclose a registration server that allows access and receives a request by a user for a new signature certificate, the registration server querying a directory to obtain information regarding the identified user, and informing a user that a new signature certificate will not be issued until the old signature certificate has been revoked in response to the server receiving information from the directory that the identified user already possesses a signature certificate, as recited in claims 1 and 9.

The Examiner finally rejects claims 1 and 9 based on Col. 8, line 50 to col. 9 line 23 of Yacobi, which discloses a certification process in which a user's electronic wallet generates a unique pair of public and private cryptographic signing keys, and submits the key pair along with user identification and initial certificate stored by the manufacturer to the bank's computer. The bank's computer compares the initial manufacturer-issued certificate to a list of initial certificates to ensure that the wallet is a tamper-resistant device, and to the hot list of bad wallets to ensure that the wallet is not a bad wallet. If the certificate checks out cleanly, the bank's computer confirms the identity of the user. If the user is present, the identification confirmation is performed using traditional methods, such as driver's license, finger prints, and so on. If the user is not present and the certification is handled remotely, the bank relies on other evidence such as a phone number, address, mother's maiden name, and so on. Following successful confirmation, the bank's computer digitally signs the packet to produce a certificate. An expiration date is attached to the certificate and the certificate is returned to the electronic wallet.

The advisory action dated May 13, 2005 (hereinafter "Advisory Action") contends that Yacobi discloses claims 1 and 9. Yacobi states that:

> "2. For non-anonymous systems at expiration, each user gets automatically a new certification, which includes the same old public key with a new expiration (unless the user asks to replace the public key for fear that it has been exposed). At each moment, each valid user has exactly one certificate. " (Col. 5, Lines 17-22).

Yacobi does not explicitly or inherently allow a user to access a registration server and state a course of action when the requesting user requests a new signature certificate without providing an old signature certificate. The certification process disclosed in Yacobi presupposes that a user will attempt to receive a certificate only when the user is in possession of an electronic wallet, and does not allow access to any user that does not posses an electronic wallet.

Yacobi also discloses a renewal process in which the electronic wallet is obligated to submit the old certificate with public and private keys prior to the expiration date to obtain a new certificate for a new expiration term. However, there is no teaching that the user is ever informed that a new certificate will not be issued until the old certificate is revoked in response to the server receiving information from a directory that the identified user already possesses a signature certificate.

Furthermore, the Advisory Action contends that the user in Yacobi is aware that a new certificate is being produced with the same old public key and a new expiration. Assuming *arguendo* that the Advisory Action is correct, it is respectfully submitted that knowledge from the user's standpoint does not teach the elements recited in claims 1 and 9, namely, a registration server that allows access and receives a request by a user for a new signature certificate, the registration server querying a directory to obtain information regarding the identified user, and informing a user that a new signature certificate will not be

issued until the old signature certificate has been revoked in response the server receiving information from the directory that the identified user already possesses a signature certificate.

Therefore, Yacobi does not teach each and every element of claims 1 and 9, and thus does not anticipate claims 1 and 9. Accordingly, it is respectfully suggested that the rejection of claims 1 and 9 is improper and should be withdrawn.

2. 35 U.S.C. §102(b) rejection of claims 5 and 13 as being anticipated by Yacobi

Claims 5 and 13 are patentable over Yacobi because Yacobi does not disclose explicitly or inherently a registration server allowing upon the registration server receiving identification information from the user and also receiving a request by the user for a new signature certificate, the registration server querying a directory containing reference information of users of the enterprise to obtain information regarding the identified user; and upon the registration server receiving information from the directory indicating that the identified user is not in the directory, the registration server informing the user that a signature certificate will not be issued thereby preventing an unauthorized user from ID spoofing to obtain a valid signature certificate.

The Examiner finally rejects claims 5 and 13 based on Col. 8, line 50 to col. 9 line 23 of Yacobi, as recited above with respect to claims 1 and 9. Yacobi discloses a certification process in which a user's electronic wallet generates a unique pair of public and private cryptographic signing keys, and submits the key pair along with user identification and initial certificate stored by the manufacturer to the bank's computer (See Yacobi, Col. 8, Line 50-Col. 9, Line 24). Yacobi, however, does not explicitly or inherently allow a user to access a registration server and state a course of action when the requesting user is not in a directory. In fact, Yacobi discloses that the electronic wallets are manufactured with a certificate registered with a certifying authority (See Yacobi, Col. 8, Lines 50-53). Consequently, in Yacobi, if a user possesses an electronic wallet, that user also possesses a certificate. The certification process disclosed in Yacobi presupposes that a user will attempt to receive a certificate only when the user is in possession of an electronic wallet, and does not allow access to any user that does not posses an electronic wallet.

Moreover, nothing in Yacobi implies that upon a registration server receiving information from a directory indicating that an identified user is not in a directory, the registration server informing the user that a signature certificate will not be issued. In Yacobi, physical possession of the wallet is necessary to activate the certification process. Thus, inherently, in Yacobi, there is no need

for the certification process to be activated when the user is not in possession of a wallet.

The Advisory Action alleges that "Once a user requests a new certificate from the bank in Yacobi's system the bank checks to make sure that the user is registered in the database and the user is who he purports to be." (See Advisory Action) Assuming *arugendo* that the Advisory action is correct, Yacobi still does not disclose a system that begins the certification process where the user is not in possession of a wallet. That is, the user discussed in the Advisory Action possesses a certificate, and whether or not that user has authority to get a new certificate is irrelevant to the method and apparatus as recited in claims 5 and 13, since the user does not need to be in possession of a signature certificate to request a new one.

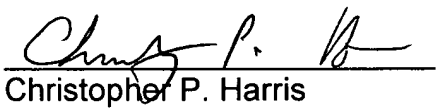
Thus, Yacobi does not disclose that upon a registration server receiving information from a directory indicating that an identified user is not in a directory, the registration server informing the user that a signature certificate will not be issued. Therefore, Yacobi does not teach each and every element of claims 5 and 13, and thus does not anticipate claims 5 and 13. Accordingly, it is respectfully suggested that the rejection of claims 5 and 13 are improper and should be withdrawn.

VIII. APPENDIX

The attached Appendix contains a copy of the claims on appeal.

Please charge any deficiency or credit any overpayment in the fees for this Appeal Brief to Deposit Account No. 20-0090.

Respectfully submitted,



Christopher P. Harris
Reg. No. 43,660

TAROLLI, SUNDHEIM, COVELL
& TUMMINO, L.L.P.
526 Superior Avenue – Suite 1111
Cleveland, Ohio 44114
(216) 621-2234
(216) 621-4072 (Facsimile)
Customer No.: 26294

Appendix

Claim 1 A method of preventing ID spoofing of a public key infrastructure system in an enterprise comprising: allowing a user to access a registration server; upon the registration server receiving identification information from the user and also receiving a request by the user for a new signature certificate, the registration server querying a directory containing reference information of users of the enterprise to obtain information regarding the identified user; and upon the registration server receiving information from the directory indicating that the identified user already possesses a signature certificate, the registration server informing the user that a new signature certificate will not be issued until the old signature certificate has been revoked, thereby preventing an unauthorized user from ID spoofing to obtain a valid signature certificate and maintaining a one-to-one correspondence between users of the enterprise and signature certificates.

Claim 5 A method of preventing ID spoofing of a public key infrastructure in an enterprise comprising: allowing a user to access a registration server; upon the registration server receiving identification information from the user and also receiving a request by the user for a new signature certificate, the registration server querying a directory containing reference information of users

of the enterprise to obtain information regarding the identified user; and upon the registration server receiving information from the directory indicating that the identified user is not in the directory, the registration server informing the user that a signature certificate will not be issued, thereby preventing an unauthorized user from ID spoofing to obtain a valid signature certificate and maintaining a one-to-one correspondence between users of the enterprise and signature certificates.

Claim 9 An apparatus for preventing ID spoofing of a public key infrastructure system in an enterprise comprising: a registration server to allow access by a user; a directory accessible by the registration server, the directory storing information regarding all users in the enterprise; wherein, upon the registration server receiving information from the user and also receiving a request by the user for a new signature certificate, the registration server querying the directory to obtain information regarding the identified user; and wherein, upon the registration server receiving information from the directory indicating that the identified user already possesses a signature certificate, the registration server informing the user that a new signature certificate will not be issued until the old signature certificate has been revoked, thereby preventing an unauthorized user from ID spoofing to obtain a valid signature certificate, such

that the directory maintains a one-to-one correspondence between the users of the enterprise and signature certificates.

Claim 13 An apparatus for preventing ID spoofing of a public key infrastructure in an enterprise comprising: a registration server to allow access by a user; a directory accessible by the registration server, the directory storing information regarding all users in the enterprise; wherein, upon the registration server receiving information from the user and also receiving a request by the user for a new signature certificate, the registration server querying the directory to obtain information regarding the identified user; and wherein, upon the registration server receiving information from the directory indicating that the identified user is not in the directory, the registration server informing the user that the user is not a valid member of the enterprise and not issue a signature certificate, such that the directory maintains a one-to-one correspondence between the users of the enterprise and signature certificates.